

Администрирование сетевых подсистем

Лабораторная работа №2

Авдадаев Джамал Геланиевич

25 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Приобретение практических навыков установки, конфигурирования и тестирования DNS-сервера, а также понимания принципов работы системы доменных имён.

Ход выполнения

Проверка работы DNS-клиента

```
[root@server.dgavdadaev.net ~]#  
[root@server.dgavdadaev.net ~]# dig www.yandex.ru  
  
; <<>> DiG 9.18.33 <<>> www.yandex.ru  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 44341  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;www.yandex.ru.                IN      A  
  
;; ANSWER SECTION:  
www.yandex.ru.                241     IN      A      5.255.255.77  
www.yandex.ru.                241     IN      A      77.88.44.55  
www.yandex.ru.                241     IN      A      77.88.55.88  
  
;; Query time: 24 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)  
;; WHEN: Tue Nov 25 09:03:35 UTC 2025  
;; MSG SIZE rcvd: 90  
  
[root@server.dgavdadaev.net ~]#
```

Рис. 1: dig www.yandex.ru

Анализ конфигурации DNS

```
[root@server.dgavdadaev.net ~]#  
[root@server.dgavdadaev.net ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
search dgavdadaev.net  
nameserver 10.0.2.3  
[root@server.dgavdadaev.net ~]# cat /etc/named.conf  
//  
// named.conf  
//  
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS  
// server as a caching only nameserver (as a localhost DNS resolver only).  
//  
// See /usr/share/doc/bind*/sample/ for example named configuration files.  
//  
  
options {  
    listen-on port 53 { 127.0.0.1; };  
    listen-on-v6 port 53 { ::1; };  
    directory      "/var/named";  
    dump-file      "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    secroots-file  "/var/named/data/named.secroots";  
    recursing-file  "/var/named/data/named.recursing";  
    allow-query     { localhost; };  
  
    /*  
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.  
    - If you are building a RECURSIVE (caching) DNS server you need to enable
```

Рис. 2: Конфигурация DNS

Анализ конфигурации DNS

```
[root@server.dgavdadaev.net ~]# cat /var/named/named.ca
;
; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>"
; configuration file of BIND domain name servers).
;
; This file is made available by InterNIC
; under anonymous FTP as
;       file           /domain/named.cache
;       on server      FTP.INTERNIC.NET
;       -OR-           RS.INTERNIC.NET
;
;       last update:    December 20, 2023
;       related version of root zone:  2023122001
;
; FORMERLY NS.INTERNIC.NET
;
.                3600000      NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000      A      198.41.0.4
A.ROOT-SERVERS.NET. 3600000      AAAA   2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                3600000      NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000      A      170.247.170.2
B.ROOT-SERVERS.NET. 3600000      AAAA   2801:1b8:10::b
;
; FORMERLY C.PSI.NET
;
```

Анализ конфигурации DNS

```
[root@server.dgavdadaev.net ~]#  
[root@server.dgavdadaev.net ~]# cat /var/named/named.localhost  
$TTL 1D  
@      IN SOA  @ rname.invalid. (  
                                0      ; serial  
                                1D     ; refresh  
                                1H     ; retry  
                                1W     ; expire  
                                3H )   ; minimum  
  
      NS      @  
      A      127.0.0.1  
      AAAA    ::1  
[root@server.dgavdadaev.net ~]# cat /var/named/named.loopback  
$TTL 1D  
@      IN SOA  @ rname.invalid. (  
                                0      ; serial  
                                1D     ; refresh  
                                1H     ; retry  
                                1W     ; expire  
                                3H )   ; minimum  
  
      NS      @  
      A      127.0.0.1  
      AAAA    ::1  
      PTR     localhost.  
[root@server.dgavdadaev.net ~]#
```


Сравнение работы внешнего и локального DNS

```
[root@server.dgavdadaev.net ~]# dig @127.0.0.1 www.yandex.ru
;; communications error to 127.0.0.1#53: timed out

; <<>> DiG 9.18.33 <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54610
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 96a73093f679ea36010000006925723dbf6bc8d8243e3719 (good)
;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                 600     IN      A      77.88.44.55
www.yandex.ru.                 600     IN      A      77.88.55.88
www.yandex.ru.                 600     IN      A      5.255.255.77

;; Query time: 1636 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Nov 25 09:09:17 UTC 2025
;; MSG SIZE rcvd: 118

[root@server.dgavdadaev.net ~]#
```

Настройка локального DNS сервера

```
[root@server.dgavdadaev.net ~]# nmcli connection edit eth0

===| nmcli interactive connection editor |===

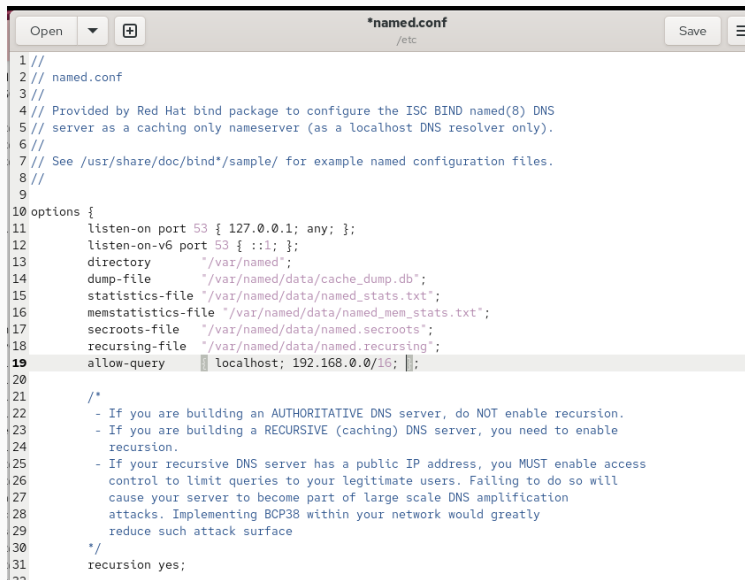
Editing existing '802-3-ethernet' connection: 'eth0'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, ethtool, match, ipv4
, ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (e292e83a-7750-4087-b4e1-a998fc55c0ea) successfully updated.
nmcli> quit
[root@server.dgavdadaev.net ~]# systemctl restart NetworkManager
[root@server.dgavdadaev.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search dgavdadaev.net
nameserver 127.0.0.1
[root@server.dgavdadaev.net ~]#
```

Рис. 6: Настройка NetworkManager

Изменение named.conf



```
1 //
2 // named.conf
3 //
4 // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
5 // server as a caching only nameserver (as a localhost DNS resolver only).
6 //
7 // See /usr/share/doc/bind*/sample/ for example named configuration files.
8 //
9
10 options {
11     listen-on port 53 { 127.0.0.1; any; };
12     listen-on-v6 port 53 { ::1; };
13     directory "/var/named";
14     dump-file "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     secroots-file "/var/named/data/named.secroots";
18     recursing-file "/var/named/data/named.recursing";
19     allow-query { localhost; 192.168.0.0/16; };
20
21     /*
22      - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
23      - If you are building a RECURSIVE (caching) DNS server, you need to enable
24        recursion.
25      - If your recursive DNS server has a public IP address, you MUST enable access
26        control to limit queries to your legitimate users. Failing to do so will
27        cause your server to become part of large scale DNS amplification
28        attacks. Implementing BCP38 within your network would greatly
29        reduce such attack surface
30     */
31     recursion yes;
32 }
```

Проверка работы UDP-порта 53

```
[root@server.dgavdadaev.net ~]# gedit /etc/named.conf
[root@server.dgavdadaev.net ~]#
[root@server.dgavdadaev.net ~]# firewall-cmd --add-service=dns
success
[root@server.dgavdadaev.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.dgavdadaev.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs:
Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc:
Output information may be incomplete.
avahi-daemon 880      avahi  12u    IPv4      8003      0t0      UDP *:mdns
avahi-daemon 880      avahi  13u    IPv6      8004      0t0      UDP *:mdns
chrony       918      chrony 5u     IPv4      7946      0t0      UDP localhost:323
chrony       918      chrony 6u     IPv6      7947      0t0      UDP localhost:323
named        15480    named  25u    IPv4      75689     0t0      UDP localhost:doma
in
named        15480    named  26u    IPv4      75690     0t0      UDP localhost:doma
in
named        15480    named  31u    IPv6      75693     0t0      UDP localhost:doma
in
named        15480    named  32u    IPv6      75694     0t0      UDP localhost:doma
in
named        15480 15481 isc-net-0 named  25u    IPv4      75689     0t0      UDP localhost:doma
in
named        15480 15481 isc-net-0 named  26u    IPv4      75690     0t0      UDP localhost:doma
in
named        15480 15481 isc-net-0 named  31u    IPv6      75693     0t0      UDP localhost:doma
```

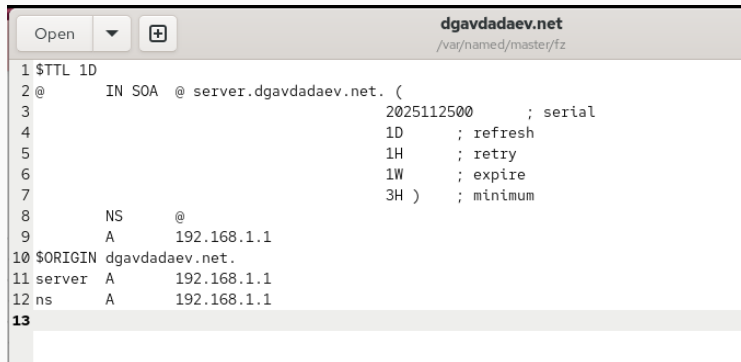
Рис. 8: Проверка UDP 53

Создание файла зон



The screenshot shows a text editor window with a title bar that includes the text "dgavdadaev.net" and a file path "/etc/named". The editor contains a BIND configuration file with the following content:

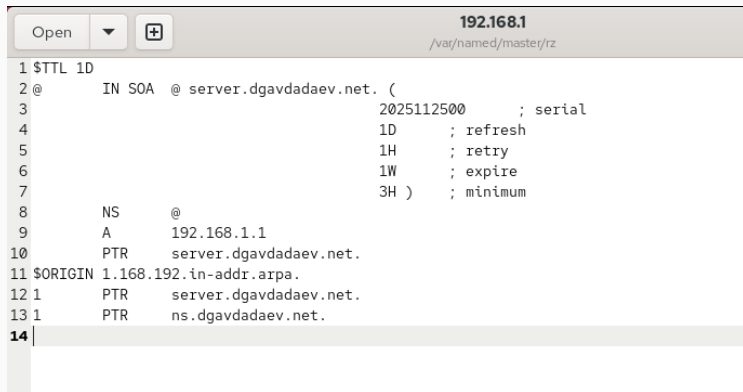
```
1 // named.rfc1912.zones:
2 //
3 // Provided by Red Hat caching-nameserver package
4 //
5 // ISC BIND named zone configuration for zones recommended by
6 // RFC 1912 section 4.1 : localhost TLDs and address zones
7 // and https://tools.ietf.org/html/rfc6303
8 // (c)2007 R W Franks
9 //
10 // See /usr/share/doc/bind*/sample/ for example named configuration files.
11 //
12 // Note: empty-zones-enable yes; option is default.
13 // If private ranges should be forwarded, add
14 // disable-empty-zone "."; into options
15 //
16
17 zone "dgavdadaev.net" IN {
18     type master;
19     file "master/fz/dgavdadaev.net";
20     allow-update { none; };
21 };
22
23 zone "1.168.192.in-addr.arpa" IN {
24     type master;
25     file "master/rz/192.168.1";
26     allow-update { none; };
27 };
```



The screenshot shows a DNS configuration window for the domain **dgavdadaev.net**. The window has a title bar with "Open", a dropdown arrow, and a plus icon. Below the title bar, the path `/var/named/master/fz` is displayed. The main area contains a list of DNS records, each preceded by a line number from 1 to 13. The records are as follows:

- 1 `$TTL 1D`
- 2 `@ IN SOA @ server.dgavdadaev.net. (`
- 3 `2025112500 ; serial`
- 4 `1D ; refresh`
- 5 `1H ; retry`
- 6 `1W ; expire`
- 7 `3H) ; minimum`
- 8 `NS @`
- 9 `A 192.168.1.1`
- 10 `$ORIGIN dgavdadaev.net.`
- 11 `server A 192.168.1.1`
- 12 `ns A 192.168.1.1`
- 13 (empty line)

Рис. 10: Прямая зона



The screenshot shows a configuration window for the reverse zone 192.168.1. The window has a title bar with '192.168.1' and a path '/var/named/master/rz'. Below the title bar is a toolbar with 'Open', a dropdown arrow, and a '+' icon. The main area contains a BIND configuration file snippet for a reverse zone.

```
1 $TTL 1D
2 @      IN SOA  @ server.dgavdadaev.net. (
3                                     2025112500      ; serial
4                                     1D              ; refresh
5                                     1H              ; retry
6                                     1W              ; expire
7                                     3H )            ; minimum
8      NS      @
9      A        192.168.1.1
10     PTR      server.dgavdadaev.net.
11 $ORIGIN 1.168.192.in-addr.arpa.
12 1        PTR      server.dgavdadaev.net.
13 1        PTR      ns.dgavdadaev.net.
14 |
```

Рис. 11: Обратная зона

Перезапуск службы named

```
[root@server.dgavdadaev.net rz]#  
[root@server.dgavdadaev.net rz]# systemctl restart named  
[root@server.dgavdadaev.net rz]# systemctl status named  
● named.service - Berkeley Internet Name Domain (DNS)  
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)  
   Active: active (running) since Tue 2025-11-25 09:29:33 UTC; 1s ago  
 Invocation: c4c76de801434517b41f6579e61d8ff7  
    Process: 18752 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/bin/named-checkc  
    Process: 18754 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)  
   Main PID: 18756 (named)  
      Tasks: 6 (limit: 10381)  
     Memory: 5.2M (peak: 5.8M)  
        CPU: 22ms  
    CGroup: /system.slice/named.service  
            └─18756 /usr/sbin/named -u named -c /etc/named.conf
```

Рис. 12: Статус named

Проверка зоны dig

```
[root@server.dgavdadaev.net ~]#  
[root@server.dgavdadaev.net ~]# dig ns.dgavdadaev.net  
  
; <<>> DiG 9.18.33 <<>> ns.dgavdadaev.net  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51482  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: 70705e1b8be549e801000000692577c8f4108f038f9ab23a (good)  
;; QUESTION SECTION:  
ns.dgavdadaev.net.          IN      A  
  
;; ANSWER SECTION:  
ns.dgavdadaev.net.          86400   IN      A      192.168.1.1  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)  
;; WHEN: Tue Nov 25 09:32:56 UTC 2025  
;; MSG SIZE rcvd: 90  
  
[root@server.dgavdadaev.net ~]#
```

Проверка работы host

```
[root@server.dgavdadaev.net ~]#
[root@server.dgavdadaev.net ~]# host -l dgavdadaev.net
dgavdadaev.net name server dgavdadaev.net.
dgavdadaev.net has address 192.168.1.1
ns.dgavdadaev.net has address 192.168.1.1
server.dgavdadaev.net has address 192.168.1.1
[root@server.dgavdadaev.net ~]# host -a dgavdadaev.net
Trying "dgavdadaev.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50088
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
dgavdadaev.net.                IN      ANY

;; ANSWER SECTION:
dgavdadaev.net.                86400   IN      SOA      dgavdadaev.net. server.dgavdadaev.net. 2025112500 86400 3600 604800
10800
dgavdadaev.net.                86400   IN      NS       dgavdadaev.net.
dgavdadaev.net.                86400   IN      A        192.168.1.1

Received 105 bytes from 127.0.0.1#53 in 1 ms
[root@server.dgavdadaev.net ~]# host -t A dgavdadaev.net
dgavdadaev.net has address 192.168.1.1
[root@server.dgavdadaev.net ~]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.dgavdadaev.net.
1.1.168.192.in-addr.arpa domain name pointer ns.dgavdadaev.net.
[root@server.dgavdadaev.net ~]#
```

Рис. 14: host проверка

```
[root@server.dgavdadaev.net fz]#  
[root@server.dgavdadaev.net fz]# cd /vagrant/  
[root@server.dgavdadaev.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named  
[root@server.dgavdadaev.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master  
[root@server.dgavdadaev.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/  
[root@server.dgavdadaev.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/  
[root@server.dgavdadaev.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/  
[root@server.dgavdadaev.net vagrant]# touch dns.sh  
[root@server.dgavdadaev.net vagrant]# █
```

Рис. 15: Файлы в /vagrant

Создание provisioning-скрипта dns.sh

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install bind bind-utils
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/dns/etc/* /etc
7  cp -R /vagrant/provision/server/dns/var/named/* /var/named
8  chown -R named:named /etc/named
9  chown -R named:named /var/named
10 restorecon -vR /etc
11 restorecon -vR /var/named
12 echo "Configure firewall"
13 firewall-cmd --add-service=dns
14 firewall-cmd --add-service=dns --permanent
15 echo "Tuning SELinux"
16 setsebool named_write_master_zones 1
17 setsebool -P named_write_master_zones 1
18 echo "Change dns server address"
19 nmcli connection edit "eth0" <<EOF
20     remove ipv4.dns
21     set ipv4.ignore-auto-dns yes
22     set ipv4.dns 127.0.0.1
23     save
24     quit
25 EOF
26 systemctl restart NetworkManager
27 echo "Start named service"
28 systemctl enable named
29 systemctl start named
```

Выводы

Настроены прямая и обратная DNS-зоны, изменены параметры BIND, восстановлены права и контекст SELinux, проверена корректность работы DNS-службы.

С помощью `dig` и `host` подтверждено функционирование сервера имён.

Конфигурация перенесена в каталог Vagrant для автоматизированного развёртывания.